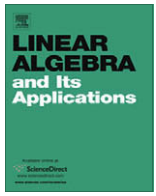
Linear Algebra and its Applications 431 (2009) 39–55

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa



Supernormal mappings: Part 1. Orthogonally indecomposable modules and applications

Olaf v. Grudzinski, Frieder Knüppel*, Klaus Nielsen

Mathematisches Seminar, Rechenzentrum der Universität Kiel, Ludewig-Meyn-Straße 4, D-24098 Kiel, Germany

ARTICLE INFO

Article history:
Received 22 May 2008
Accepted 8 February 2009
Available online 19 March 2009

Submitted by Eva Zerz

AMS classification:
20G15
14L35
15A63
15A23

Keywords:
Normal forms
Supernormal mappings
Polynomially normal mappings
Normal mappings
Hermitean forms
Unitary groups
Orthogonal groups
Symplectic groups
Classical groups
Adjoint mappings
Self-adjoint mappings

ABSTRACT

Let V be a finite-dimensional vector space over a field and $f : V \times V \to K$ a regular ε, $^-$-hermitian form. A linear mapping $\pi : V \to V$ with adjoint mapping π^*, i.e. $f(v\pi, w) = f(v, w\pi^*)$ for all $v, w \in V$, is called supernormal or polynomially normal or simply s-normal if $s(\pi) = \pi^*$ holds true for some polynomial $s \in K[x]$. If π is a unitary transformation or if π is self-adjoint or if π is anti-self-adjoint then π is s-normal. For s-normal mappings π a classification of orthogonally indecomposable π-modules is obtained. The classification distinguishes four types and depends on the form f, the minimum polynomial of π and whether $\pi^* - \pi$ is nilpotent or not. We prove a uniqueness statement for orthogonal decompositions (into orthogonally indecomposable modules) of similar s-normal mappings. As an application we generalize the fact that in an orthogonal group each element is a product of two involutions. In the generalized setting both factors are self-adjoint or anti-self-adjoint and the first one is an involution. The last section establishes a decomposition of V into orthogonally indecomposable π-modules such that each π-module is also invariant under both given factors. Part 2 will be devoted to isometric similarity of s-normal mappings.

* Corresponding author.
E-mail addresses: grudzinski@math.uni-kiel.de (O.v. Grudzinski), knueppel@math.uni-kiel.de (F. Knüppel), nielsen@rz.uni-kiel.de (K. Nielsen).

0024-3795/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2009.02.004

1. Basic assumptions and introduction

(**A**) **Basic assumptions and notations**. Let V be a finite-dimensional vector space over a field K.
Let $\pi : V \to V$ be a linear mapping. A π-module is a subspace U of V such that $U\pi \subseteq U$.
Let $\mathrm{mip}\pi$ denote the minimum polynomial and define
$P(\pi) := \{p \in K[x] \mid p \text{ is monic, irreducible and } p \mid \mathrm{mip}\pi\}$.
Further, for $q \in K[x]$ let

$$V_\pi(q) := \bigcup_{k\in\mathbb{N}} \mathrm{kernel} q^k(\pi).$$

If q is prime to $\mathrm{mip}\pi$ then $V_\pi(q) = 0$. If $q \in P(\pi)$ and $q^k \mid \mathrm{mip}\pi$ and $q^{k+1} \nmid \mathrm{mip}\pi$ then $V_\pi(q) = \mathrm{kernel} q^k(\pi)$.

Lemma 1.1 (**primary decomposition**). *For a linear mapping $\pi : V \to V$ the following decomposition into non-zero π-modules is called the primary decomposition into π-modules.*

$$V = \bigoplus_{p\in P(\pi)} V_\pi(p).$$

(**B**) **Additional basic assumption**. Let $\bar{}: K \to K$ be an involutory automorphism of K (id_K not excluded) and $\varepsilon \in K$ such that $\varepsilon\bar{\varepsilon} = 1$. Let $f : V \times V \to K$ be an $\varepsilon, \bar{}$-hermitian form (also called an ε, $\bar{}$-hermitian sesquilinear form).

This requires additivity in both components and $f(b,a) = \varepsilon\overline{f(a,b)}$ and $f(\lambda a, b) = \lambda \cdot f(a,b)$ for all $a, b \in V$ and $\lambda \in K$. It follows that $f(a, \lambda b) = \bar{\lambda} \cdot f(a,b)$.

We will further assume that f is regular, i.e.
$V^\perp := \{v \in V \mid f(v,w) = 0 \quad \text{for all } w \in V\} = \{0\}$.

Observation 1.2. Each linear mapping $\pi : V \to V$ determines a unique linear mapping $\pi^* : V \to V$ such that $f(v, w\pi) = f(v\pi^*, w)$ for all $v, w \in V$, called the adjoint to π.

We collect some basic properties.

Lemma 1.3. $(\pi^*)^* = \pi$; $(\pi\psi)^* = \psi^*\pi^*$; $(\pi + \psi)^* = \pi^* + \psi^*$;
$q(\pi)^* = \bar{q}(\pi^*)$ *for each* $q \in K[x]$; *in particular* $(\lambda\pi)^* = \bar{\lambda}\pi^*$;
$\mathrm{mip}(\pi^*) = \overline{\mathrm{mip}(\pi)}$; *in particular*, $P(\pi^*) = \overline{P(\pi)}$.

Lemma 1.4. *Let U be a subspace of V. Then U is a π-module if and only if $U^\perp$ is a π^*-module.*

A subspace U is called regular if the radical $\mathrm{rad}U := U \cap U^\perp = \{0\}$, i.e. $f|_{U\times U}$ is regular.
Note that U is regular if and only if $V = U \dotplus U^\perp$. The symbol $\dotplus$ stands for $\oplus$ and $\perp$.

Lemma 1.5 (**perpendicular-lemma**). *Let $p, q \in K[x]$ and p prime to q. Then $V_\pi(p) \perp V_{\pi^*}(\bar{q})$.*

Proof. Let $u \in V_\pi(p)$ and $v \in V_{\pi^*}(\bar{q})$. Then $up^k(\pi) = 0 = v\bar{q}^l(\pi^*)$ for some $k, l \in \mathbb{N}$. The assumption yields $r, t \in K[x]$ such that $rp^k + tq^l = 1$. Hence $u = ut(\pi)q^l(\pi)$. Using Lemma 1.3 we conclude that $f(u,v) = f(ut(\pi)q^l(\pi), v) = f(ut(\pi), v\bar{q}^l(\pi^*)) = 0$. □

Proposition 1.6 (**compare [13]**). *Let $\pi, \varphi : V \to V$ be linear mappings. The following properties are equivalent.*
(i) *$\pi\varphi = \varphi\pi$ and each π-module is a φ-module.*
(ii) *$\pi\varphi = \varphi\pi$ and if $V = U \oplus W$ where U, W are π-modules and U is π-cyclic then U is a φ-module.*
(iii) *If $\psi : V \to V$ is linear and $\pi\psi = \psi\pi$ then $\varphi\psi = \psi\varphi$.*
(iv) *$\varphi = s(\pi)$ for some $s \in K[x]$.*

Proof. The statements (i) ⇒ (ii), and (iv) ⇒ (i), and (iv) ⇒ (iii) are obvious.
Proof of (ii) ⇒ (iv).

Consider all decompositions $V = U \oplus W_1 \oplus \cdots \oplus W_k$ where $U = \langle u \rangle_\pi$ and each W_i are π-cyclic modules. Take such a decomposition where $\dim U$ is maximal. Then $\mathrm{mip}\pi = \mathrm{mip}\pi|_U$. Statement (ii) yields that $u\varphi \in U$. Hence some polynomial p satisfies $up(\pi) = u\varphi$. If $V = U$ this yields that $\varphi = p(\pi)$ and (iv) follows. Else put $W := W_1 = \langle w \rangle_\pi$ and $Z := \langle u + w \rangle_\pi$. Statement (ii) provides $p_Z, p_W \in K[x]$ such that $(u+w)p_Z(\pi) = (u+w)\varphi$ and $wp_W(\pi) = w\varphi$. Then $up_Z(\pi) + wp_Z(\pi) = (u+w)p_Z(\pi) = (u+w)\varphi = u\varphi + w\varphi = up(\pi) + wp_W(\pi)$. As $U \cap W = \{0\}$ this yields $up_Z(\pi) = up(\pi)$ and $wp_Z(\pi) = wp_W(\pi)$. Hence $p_Z(\pi)$ coincides on U with $p(\pi)$ and on W with $p_W(\pi)$. Therefore, $\mathrm{mip}\pi|_U = \mathrm{mip}\pi$ divides $p - p_Z$. As $\mathrm{mip}\pi|_W$ divides $\mathrm{mip}\pi$ we conclude that $\mathrm{mip}\pi|_W$ divides $p - p_Z$. Hence $w\varphi = wp_W(\pi) = wp_Z(\pi) = wp(\pi)$. So $\varphi|_W = p(\pi)|_W$. As this argument applies to each W_i we proved that $\varphi = p(\pi)$.

Proof of (iii) $\Rightarrow$ (ii).

Clearly, (iii) implies that $\pi\varphi = \varphi\pi$.

Now let $V = U \oplus W$ where U, W are π-modules and U is π-cyclic. We must prove $U\varphi \subseteq U$. Let σ denote the canonical projection to U (based on the decomposition $V = U \oplus W$). Then $\pi\sigma = \sigma\pi$, hence $\varphi\sigma = \sigma\varphi$. Therefore, $U\varphi = U\sigma\varphi = U\varphi\sigma \subseteq U$. □

Corollary 1.7 (**defining properties of supernormal mappings**). *Let $\pi : V \to V$ be a linear mapping. The following statements are equivalent.*

(j) *$\pi\pi^* = \pi^*\pi$ and each π-module is a π^*-module.*

(jj) *If $\psi : V \to V$ is linear and $\pi\psi = \psi\pi$ then $\pi^*\psi = \psi\pi^*$.*

(jjj) *$\pi^* = s(\pi)$ for some $s \in K[x]$.*

Definition 1.8 (**s-normal mappings**). A linear mapping $\pi : V \to V$ is called *s*-normal if $s \in K[x]$ satisfies $s(\pi) = \pi^*$. We call π also supernormal or *s*-normal if π fulfills one of the equivalent conditions in the previous corollary.

If π is an *s*-normal mapping and $r \in K[x]$ is congruent to s modulo $\mathrm{mip}\pi$ then π is also *r*-normal.

Linear mappings that satisfy $\pi^*\pi = \pi\pi^*$ are called normal mappings. Each *s*-normal mapping is a normal mapping.

Examples of s-normal mappings are unitary transformations,[1] self-adjoint (also called symmetric) transformations ($\pi^* = \pi$), anti-self-adjoint transformations ($\pi^* = -\pi$).

For each kind of these transformations orthogonal decompositions into orthogonally indecomposable π-modules have been studied by G. Williamson, Zassenhaus, Springer and Steinberg, G. E. Wall (see bibliography). A more recent treatment for orthogonal and symplectic mappings is given in [10,11]. Huppert extended his studies to unitary transformations in [12]. For the reals and the complex numbers s-normal mappings were treated in [16].

The present article studies orthogonal decompositions into π-modules for arbitrary *s*-normal mappings over any field ($\mathrm{char}K = 2$ occasionally excluded), including the above-mentioned results in a unified approach. In a second part we will discuss isometric similarity of *s*-normal mappings.

The first author studied *s*-normal mappings in an unpublished manuscript [7].

Observation 1.9. For a linear mapping $\pi : V \to V$ let $V = U_1 \perp U_2$ be an orthogonal decomposition into π-modules.

(a) If π is *s*-normal then the restrictions π_i to U_i are *s*-normal.

(b) Suppose that the restrictions π_i are s_i-normal. If $\mathrm{mip}\pi_2 | s_1 - s_2$ (in particular if $s_1 = s_2$) or if $\mathrm{mip}\pi_1$ is prime to $\mathrm{mip}\pi_2$ then π is s-normal.

Proof of (b). If $\mathrm{mip}\pi_2 | s_1 - s_2$ put $s := s_1$. Else apply the chinese remainder theorem: we obtain a polynomial s such that $s \equiv s_1 \bmod \mathrm{mip}\pi_1$ and $s \equiv s_2 \bmod \mathrm{mip}\pi_2$. Then $u_i\pi^* = u_i\pi_i^* = u_i s_i(\pi_i) = u_i s(\pi_i)$ for each $u_i \in U_i$. □

[1] Observe that $\pi^{-1} \in K[\pi]$ for each $\pi \in \mathrm{GL}(V)$.

Observation 1.10 (**matrix formulation**). Take a basis $e_1, \ldots, e_n$ for V.

The matrix $F := (f(e_i, e_j))$ satisfies $F^t = \varepsilon\overline{F}$ where F^t denotes the transpose. Then $f(v, w) = vF\bar{w}^t$ where we identify $v = v_1e_1 + \cdots + v_ne_n \in V$ with its coordinate $1 \times n$-matrix $(v_1, \ldots, v_n)$.

For a linear mapping $\pi : V \to V$ let A denote the matrix given by $e_i\pi = \sum_j a_{ij}e_j$. The adjoint π^* corresponds to the matrix $A^* = F\overline{A}^tF^{-1}$.

As A^t is similar to A we conclude:

The matrix A^* of the adjoint π^* is similar to $\overline{A}$ (where A is the matrix of π). In particular, if $\bar{} = \mathrm{id}_K$ then φ^* is similar to φ.

2. First results on supernormal mappings

Assumption. In the sequel let $s \in K[x]$. We will assume that π is an s-normal mapping.

Notations. For $r, s \in K[x]$ let $r \circ s$ denote the polynomial obtained by replacing each x in r by s (corresponding to the composition of mappings).

Put $q^* := \bar{q} \circ s$ for each $q \in K[x]$.

Observation 2.1. (a) $(q(\pi))^* = \bar{q}(\pi^*) = \bar{q} \circ s(\pi) = q^*(\pi)$ for all $q \in K[x]$. The mapping * is a homomorphism of the ring $K[x]$. The restriction to K is the automorphism $\bar{}$.
Further, $V_{\pi^*}(\bar{q}) = V_\pi(q^*)$.
If $p, q \in K[x]$ and p is prime to q then $V_\pi(p) \perp V_\pi(q^*)$.
(b) The identity $\bar{s}(\pi^*) = \pi^{**} = \pi$ (see Lemma 1.3) proves that π^* is an $\bar{s}$-normal mapping. In particular, $K[\pi] = K[\pi^*]$ and $\mathrm{mip}\pi|\bar{s} \circ s - x$.
(c) The lattice $\mathfrak{L}$ of π-modules coincides with the lattice of π^*-modules. If $U \in \mathfrak{L}$ then $U^\perp \in \mathfrak{L}$.

Proof. The identity in (a) follows from Lemma 1.3 and it yields that $V_{\pi^*}(\bar{q}) = V_\pi(q^*)$. This result and Lemma 1.5 prove the last assertion in (a). The other facts are obvious from the definitions and Corollary 1.7. □

Let $\mathfrak{L}$ denote the **lattice** of π-modules (which coincides with the lattice of π^*-modules). For $U \in \mathfrak{L}$ let $\mathfrak{L}(U)$ denote the sub-lattice of submodules of U.

Definition 2.2. For $p, s \in K[x]$ where p is monic and $p = (x - \lambda_1) \times \cdots \times (x - \lambda_n)$ in a splitting field over K define

$$p_s := (x - s(\lambda_1)) \times \cdots \times (x - s(\lambda_n)).$$

Let $\mathrm{char}\,\psi$ denote the characteristic polynomial of a linear mapping ψ.

Lemma 2.3. (a) *Let $p, q, s, t \in K[x]$ such that p, q are monic. Then $(p \cdot q)_s = p_s \cdot q_s$ and $(p_s)_t = p_{t\circ s}$.*
(b) *If $\psi : V \to V$ is linear and $s \in K[x]$ and $p := \mathrm{char}\,\psi$ then $p_s = \mathrm{char}(s(\psi))$. In particular, $p_s \in K[x]$ for all $p, s \in K[x]$.*

Proof of (b). Let $A \in K^{n\times n}$ be the matrix of ψ (in a basis for V) and let L be a splitting field for p over K. Then A is in $L^{n\times n}$ similar to an upper triangular matrix with entries $\lambda_1, \ldots, \lambda_n$ in the diagonal. Hence $s(A)$ is similar to an upper triangular matrix with entries $s(\lambda_1), \ldots, s(\lambda_n)$ in the diagonal. In particular, $\mathrm{char}(s(A)) = p_s$. □

Observation 2.4. $U \in \mathfrak{L}$ is an indecomposable π-module if and only if $\mathfrak{L}(U)$ is a chain. The atoms of $\mathfrak{L}$ are precisely the cyclic π-modules with minimum-polynomial in $P(\pi)$ (and also the cyclic π^*-modules with minimum-polynomial in $P(\pi^*)$).

Indeed, if U is indecomposable then U is a π-cyclic module and $\mathrm{mip}\pi = p^k$ for some $p \in P(\pi)$ and positive integer k, hence $\mathfrak{L}(U) = \{Up(\pi)^i \mid i \in \{0,\ldots,k\}\}$. Conversely, if $\mathfrak{L}(U)$ is a chain then U is obviously indecomposable.

Proposition 2.5 (**and definition of the tilde involution**).
(a) *Let $U \in \mathfrak{L}$ be an atom. Then $p := \mathrm{mip}(\pi|_U) \in P(\pi)$ and $p_s = \mathrm{mip}(\pi^*|_U) \in P(\pi^*)$, hence $\tilde{p} := \overline{p_s} \in P(\pi)$.*
(b) *The tilde mapping $\tilde{}: P(\pi) \to P(\pi)$, $p \mapsto \tilde{p} := \overline{p_s}$, is an involution.*
(c) *For each $p \in P(\pi)$, $\tilde{p}$ is the only polynomial $\in P(\pi)$ that divides p^*.*

Proof of (a). An atom $U \in \mathfrak{L}$ is a cyclic π-module such that $\mathrm{mip}(\pi|_U) \in P(\pi)$. The analogue statement holds true for π^*. Lemmas 1.3 and 2.3 yield the assertion.

Proof of (b). The tilde mapping is well-defined, see (a). Let $p \in P(\pi)$. Put $q := \tilde{p}$. In order to prove that $\tilde{q} = p$ take $U \in \mathfrak{L}$ as in (a). Then $\bar{q} = \mathrm{mip}(\pi^*|_U)$, hence the minimum polynomial of $\bar{s}(\pi^*)|_U = \pi|_U$ is $\bar{q}_{\bar{s}} = \overline{q_s}$, see Lemma 2.3. So $p = \overline{q_s} = \tilde{q}$. We proved that the tilde mapping is an involution.

Proof of (c). Take U as in (a) and (b). Then $U\tilde{p}^*(\pi) = U\bar{\tilde{p}}(\pi^*) = 0$ (see (a)). Hence $p \mid \tilde{p}^*$.

Now assume that $q \mid \tilde{p}^*$ where $p, q \in P(\pi)$. Take an atom $W \in \mathfrak{L}$ such that $Wq(\pi) = 0$. Then (a) yields $W\bar{\tilde{q}}(\pi^*) = 0$. From $q \mid \tilde{p}^*$ we obtain $W\tilde{p}^*(\pi) = 0$, hence $W\bar{\tilde{p}}(\pi^*) = 0$. As $\bar{\tilde{p}}, \bar{\tilde{q}} \in P(\pi^*)$ it follows that $p = q$. □

We give a visual interpretation of the tilde mapping. A π-coloring and a π^*-coloring is assigned to the atoms of $\mathfrak{L}$. The set of colors is $P(\pi)$; the π-color of the atom U is $p = \mathrm{mip}(\pi|_U)$; the π^*-color of the atom U is $\tilde{p} = \overline{p_s} = \overline{\mathrm{mip}(\pi^*|_U)}$.

Corollary 2.6. *$V_\pi(p) = V_{\pi^*}(p_s) = V_{\pi^*}(\bar{\tilde{p}}) = V_\pi(\tilde{p}^*)$ for each $p \in P(\pi)$.*

Lemma 2.7. *If $p, q \in P(\pi)$ and $p \neq q$ then $V_\pi(p) \perp V_\pi(\tilde{q})$.*
In particular, if $p \in P(\pi)$ and $p \neq \tilde{p}$ then $V_\pi(p)$ is totally isotropic.
If $p, q \in P(\pi)$ and $\{p, \tilde{p}\} \neq \{q, \tilde{q}\}$ then $V_\pi(p) + V_\pi(\tilde{p}) \perp V_\pi(q) + V_\pi(\tilde{q})$.

Proof. The previous corollary yields that $V_\pi(\tilde{q}) = V_{\pi^*}(\bar{q})$ and Lemma 1.5 proves the first assertion. The second one follows immediately. □

Proposition 2.8 (**primary orthogonal decomposition of s-normal mappings**). *Put $\prod := \{\{p, \tilde{p}\} \mid p \in P, p \neq \tilde{p}\}$. Then*

$$V = \left[\textcircled{\perp}_{p \in P, p = \tilde{p}} V_\pi(p)\right] \textcircled{\perp} \left[\textcircled{\perp}_{\{p,\tilde{p}\} \in \prod} V_\pi(p) \oplus V_\pi(\tilde{p})\right].$$

If $p \in P$ and $p = \tilde{p}$ then $V_\pi(p)$ is regular.
If $p \in P$ and $p \neq \tilde{p}$ then $V_\pi(p) \oplus V_\pi(\tilde{p})$ is a regular subspace; $V_\pi(p)$ and $V_\pi(\tilde{p})$ are totally isotropic (in particular $\dim V_\pi(p) = \dim V_\pi(\tilde{p})$*).*

Proof. The primary decomposition Lemma 1.1 reads

$$V = \bigoplus_{p \in P} V_\pi(p) = \left[\oplus_{p \in P, p = \tilde{p}} V_\pi(p)\right] \oplus \left[\oplus_{\{p,\tilde{p}\} \in \prod} V_\pi(p) \oplus V_\pi(\tilde{p})\right].$$

The last statement in the previous lemma provides the $\perp$-terms.
In a direct orthogonal decomposition of a regular space (V, f) all summands are regular.
The last assertion follows from the first statement in Lemma 2.7. □

Proposition 2.9 (**additional statements to previous result**). *Let $p \in P(\pi)$.*
If $k, l \in \mathbb{N}$ are the minimal numbers such that $V_\pi(p)p(\pi)^k = 0$ respectively $V_\pi(\tilde{p})\tilde{p}(\pi)^l = 0$ then $k = l$.
If $i, j \in \mathbb{N}_0$ and $i + j \geqslant k$ then $V_\pi(p)p(\pi)^i \perp V_\pi(\tilde{p})\tilde{p}(\pi)^j$.

Proof. We may assume that $k \leqslant l$ and prove the second assertion. Let $a \in V_\pi(p)$ and $b \in V_\pi(\tilde{p})$. Then (+) $f(ap(\pi)^i, b\tilde{p}(\pi)^j) = f(ap(\pi)^i\tilde{p}^*(\pi)^j, b) = 0$ as $i+j \geqslant k$ and $p \mid \tilde{p}^*$ (see Proposition 2.5) and $ap(\pi)^k = 0$.

The special case $i = 0$ and $j = k$ states that $V_\pi(p) \perp V_\pi(\tilde{p})\tilde{p}(\pi)^k$. If $p = \tilde{p}$ then $V_\pi(p)$ is regular (see Proposition 2.8) and it follows that $V_\pi(\tilde{p})\tilde{p}(\pi)^k = 0$. Else $V_\pi(p) \oplus V_\pi(\tilde{p})$ is regular and $V_\pi(\tilde{p})$ is totally isotropic. Again we conclude that $V_\pi(\tilde{p})\tilde{p}(\pi)^k = 0$. Hence $l \leqslant k$ and thus $l = k$. □

The previous proposition implies that the maximum length of chains in $\mathfrak{L}(V_\pi(p))$ equals the maximum length of chains in $\mathfrak{L}(V_\pi(\tilde{p}))$.

Corollary 2.10. *Let $p \in P(\pi)$, $p = \tilde{p}$ and $t \in \mathbb{N}$ such that $V_\pi(p)p(\pi)^t = 0$.*
If $i, j \in \mathbb{N}_0$ satisfy $i + j \geqslant t$ then $V_\pi(p)p(\pi)^i \perp V_\pi(p)p(\pi)^j$.
In particular, if $i \in \mathbb{N}$ such that $i \geqslant \frac{t}{2}$ then $V_\pi(p)p^i(\pi)$ is totally isotropic.

Corollary 2.11. *Let $p \in P(\pi)$, $p = \tilde{p}$ and $t \in \mathbb{N}$ the minimal number such that $V_\pi(p)p(\pi)^t = 0$. If $t \geqslant 2$ then $V_\pi(p)$ contains an isotropic vector $\neq 0$.*

Example 2.12. Suppose that $\pi^* = \pi^{-1}$ (π is a unitary transformation) and $r := \mathrm{mip}\pi = x^m + r_{m-1}x^{m-1} + \cdots + r_0$. Then $s := -r_0^{-1}(x^{m-1} + r_{m-1}x^{m-2} + \cdots + r_1) = -\frac{1}{x}(r_0^{-1} \cdot r - 1)$ fulfills $s(\pi) = \pi^{-1} = \pi^*$.

Let $q \in K[x]$ such that $q \mid r$ in $K[x]$. Then $q = (x - \lambda_1) \times \cdots \times (x - \lambda_k)$ (in an appropriate splitting field) and

$$\overline{q_s} = (x - \overline{\lambda_1}^{-1}) \times \cdots \times (x - \overline{\lambda_k}^{-1}) = \overline{q_0}^{-1} \cdot x^k \cdot \bar{q}\left(\frac{1}{x}\right).$$

A polynomial $q = x^k + q_{k-1}x^{k-1} + \cdots + q_0$ with $q_0 \neq 0$ is symmetric, i.e. $\overline{q_s} = q$, if and only if $q = \overline{q_0}^{-1} \cdot x^k \cdot \bar{q}(\frac{1}{x})$. This means that $q_0\overline{q_i} = q_{k-i}$ for $i = 0, \ldots, k$ (where $q_k = 1$).

We obtained: If $\pi^* = \pi^{-1}$ then $\mathrm{mip}\pi$ is a symmetric polynomial. Of course, this is obvious without our formalism.

Suppose that $\pi^* = \pi^{-1}$ and additionally that the minimum polynomial is $\mathrm{mip}\pi = p^t$ where p is irreducible. Suppose further that $\pi^* - \pi$ is nilpotent, i.e. $p \mid s - x$. This situation will play a role in the coming section. Then $p \mid xs - x^2$ and $0 = (xs - x^2)^t(\pi) = (1 - x^2)^t(\pi)$, hence $p \mid 1 - x^2$. We conclude that $p = x + 1$ or $p = x - 1$.

Lemma 2.13. *Let π be an s-normal mapping, $p \in P(\pi)$ and $\tilde{p} = p$.*
(a) *Let W be a π-module and $t \in \mathbb{N}$ such that $Wp(\pi)^{t-1} = 0$. Then $Vp(\pi)^{t-1} \subseteq W^\perp$.*
(b) *Let $Vp(\pi)^t = 0$. Let U be a π-module and maximal with the property that each elementary divisor of the restriction π_U is p^t. Then U is a regular subspace.*

Proof of (a). Let $v \in V$ and $w \in W$. Then $f(vp(\pi)^{t-1}, w) = f(v, wp^*(\pi)^{t-1}) = 0$.

Proof of (b). The π-module U is a direct sum of π-cyclic modules with minimum polynomials p^t. We find a decomposition $V_\pi(p) = U \oplus W$ such that W is a π-module and $Wp(\pi)^{t-1} = 0$. Statement (a) yields that $Up(\pi)^{t-1} \subseteq W^\perp$. If U is not regular then $Up(\pi)^{t-1} = \mathrm{kernel}p(\pi)|_U$ contains some vector $r \in U^\perp \setminus \{0\}$ (each minimal π-module in U is contained in $\mathrm{kernel}p(\pi)|_U$). This yields $r \in V^\perp = 0$. □

3. Orthogonally indecomposable modules

Definition 3.1. Let $\pi : V \to V$ be an s-normal mapping. A π-module U is called *orthogonally* indecomposable if U is a regular subspace and if $U = T \dotplus Z$ for π-modules T and Z implies that $T = 0$ or $Z = 0$.

Each orthogonally indecomposable π-module is an orthogonally indecomposable π^*-module and vice versa.

Remark 3.2. Let $\pi : V \to V$ be a linear mapping. A π-module U is called indecomposable if $U = T \oplus Z$ implies that $T = 0$ or $Z = 0$ for all π-modules T and Z.

The following characterization is well-known: A π-module U is an indecomposable π-module if and only if U is π-cyclic and $\mathrm{mip}\pi|_U = p^k$ for an irreducible polynomial p and $k \in \mathbb{N}_0$.

One must carefully distinguish between indecomposable π-modules and orthogonally indecomposable π-modules. A regular indecomposable π-module is orthogonally indecomposable. However, an orthogonally indecomposable π-module need not be an indecomposable π-module.

Observation 3.3. Let $\pi : V \to V$ be an s-normal mapping.

(a) V admits an orthogonal decomposition $V = V_1 \perp \cdots \perp V_k$ into orthogonally indecomposable π-modules.

(b) A regular π-module U is an orthogonally indecomposable π-module if and only if U does not contain a regular π-module $W \neq 0, U$ (otherwise $U = W \perp (U \cap W^\perp)$).

(c) If $V \neq \{0\}$ is an orthogonally indecomposable π-module then the primary orthogonal decomposition Proposition 2.8 leaves only two possibilities, namely $|P(\pi)| = 1$ or $|P(\pi)| = 2$:

(I) $P(\pi) = \{p\}$, hence $p = \tilde{p}$ and $V = V_\pi(p)$, or

(II) $P(\pi) = \{p, \tilde{p}\}$ and $p \neq \tilde{p}$, hence $V = V_\pi(p) \oplus V_\pi(\tilde{p})$.

We want to describe all orthogonally indecomposable π-modules. Due to (a) such a description provides a characterization of all s-normal mappings.

Part (c) of the observation limits the investigation to modules of type (I) or (II).

Lemma 3.4. *Let U, W be cyclic π-modules and $p \in P(\pi)$, $t \in \mathbb{N}$ such that $\mathrm{mip}\pi|_U = p^t$ and $\mathrm{mip}\pi|_W = \tilde{p}^t$ ($p = \tilde{p}$ or $p \neq \tilde{p}$). Suppose that U and W are non-regular subspaces and $Up(\pi)^{t-1} \not\subseteq W^\perp$. Then $U + W = U \oplus W$ and the π-module $U \oplus W$ is regular.*

Proof. The only minimal π-module of U is $Up(\pi)^{t-1}$; and $W\tilde{p}(\pi)^{t-1}$ is the only minimal π-module of W. Therefore, if $U \cap W \neq 0$ then $Up(\pi)^{t-1} = W\tilde{p}(\pi)^{t-1}$ and as $W\tilde{p}(\pi)^{t-1} \subseteq W^\perp$ (since W is not regular) we arrive at the contradiction $Up(\pi)^{t-1} \subseteq W^\perp$.

Now suppose that $T := U \oplus W$ is not regular. Then $T \cap T^\perp$ contains a minimal π-module of T, hence $0 \neq a + b \in T \cap T^\perp$ for some $a \in Up(\pi)^{t-1}$ and $b \in W\tilde{p}(\pi)^{t-1}$ (each minimal π-module of T is contained in $Up(\pi)^{t-1} + W\tilde{p}(\pi)^{t-1}$). If $a \neq 0$ then $a \in Up(\pi)^{t-1} \cap W^\perp$, hence $Up(\pi)^{t-1} \subseteq W^\perp$. If $b \neq 0$ then $W\tilde{p}(\pi)^{t-1} \subseteq U^\perp$ and (as $\tilde{p}|p^*$) also $Up(\pi)^{t-1} \subseteq W^\perp$. □

Corollary 3.5 (**first approach to type I modules**). *If V is an orthogonally indecomposable π-module of type (I), i.e. $V = V_\pi(p)$ where $\tilde{p} = p$, then V is an indecomposable π-module (in particular π-cyclic); or $V = U \oplus W$ where U and W are indecomposable π-modules with the same minimum polynomials p^t.*

Proof. Write $V = V_1 \oplus \cdots \oplus V_r$ where V_i are cyclic π-modules $\neq 0$. By Lemma 2.13 any two π-modules V_i have the same minimum polynomial p^t. Put $U := V_1$. If $r = 1$ there is nothing to prove, so assume $r \geqslant 2$. As V is regular and U is not regular we can assume that $Up(\pi)^{t-1} \not\subseteq W^\perp$ for $W = V_2$. Lemma 3.4 asserts that $U \oplus W$ is regular, hence $V = U \oplus W$. □

Corollary 3.6. (**description of type II modules**) *If V is an orthogonally indecomposable π-module of type (II), i.e. $V = V_\pi(p) \oplus V_\pi(\tilde{p})$ where $\tilde{p} \neq p$, then $V_\pi(p)$ is a totally isotropic cyclic π-module with minimum polynomial p^t; and $V_\pi(\tilde{p})$ is a totally isotropic cyclic π-module with minimum polynomial $\tilde{p}^t$.*

Proof. The modules $V_\pi(p)$ and $V_\pi(\tilde{p})$ are totally isotropic; see Lemma 2.7. Let p^t be the minimum polynomial of $V_\pi(p)$ and select a π-cyclic submodule U such that p^t is also the minimum polynomial of U. Then $Up(\pi)^{t-1} \not\subseteq w^\perp$ for some $w \in V$. As $V_\pi(p)$ is not regular we can assume that $w \in V_\pi(\tilde{p})$. Put $W := \langle w \rangle_\pi$. Then $\mathrm{mip}\pi_W = \tilde{p}^t$ (else $W\tilde{p}(\pi)^{t-1} = 0$, hence $Up(\pi)^{t-1} \subseteq W^\perp$). Lemma 3.4 yields that $U \oplus W$ is regular, hence the assertion. □

Proposition 3.7 (**converse to previous corollary**). *Let $\pi : V \to V$ be an s-normal mapping. Let $V = U \oplus W$ where U and W are π-cyclic modules $\neq 0$ and $\mathrm{mip}\pi|_U = p^r$ and $\mathrm{mip}\pi|_W = \tilde{p}^t$ where $p \in K[x]$ is irreducible and $\tilde{p} \neq p$. Then U and W are totally isotropic and V is an orthogonally indecomposable π-module.*

Proof. From Proposition 2.8 it follows that $U = V_\pi(p)$ and $W = V_\pi(\tilde{p})$ are totally isotropic.

Suppose that $Z \neq 0$ is a regular π-module in V. Then $V = Z \oplus T$ where $T := Z^\perp$.

We have $\mathrm{mip}\pi = p^r\tilde{p}^t$, hence $p^r \mid \mathrm{mip}\pi|_Z$ or $p^r \mid \mathrm{mip}\pi|_T$. Suppose the first statement is valid (else switch Z with T). The primary decomposition of Z supplies $Z = U' \oplus W'$ where $U' := U \cap Z$ and $W' := W \cap Z$. Clearly $p^r \mid \mathrm{mip}\pi|_{U'}$. Hence U' contains a π-cyclic subspace of dimension $\geqslant \deg p^r$. Further, $\dim U = \deg p^r$ as U is π-cyclic. So $U' = U$. Since Z is regular and U', W' are totally isotropic we obtain $\dim W' = \dim U' = \dim U = \dim W$. Hence $W' = W$ and we proved that $Z = V$. □

The previous proposition is a first approach to orthogonally indecomposable π-modules of type (I). When $\mathrm{char}K \neq 2$ we will find additional properties.

In the study of orthogonally indecomposable π-modules (where π is s-normal) the case that $\pi^* - \pi$ is nilpotent plays a special role. When $\mathrm{mip}\pi = p^t$ for an irreducible polynomial p then $\pi^* - \pi$ is nilpotent if and only if $p \mid s - x$. We will need a lemma on polynomials.

Lemma 3.8. *Let $s \in K[x]$ and t a positive integer. Suppose that $p \in K[x]$ is irreducible and $p \mid s - x$.*
If $\mathrm{char}K \neq 2$ and $p^t \mid s \circ s - x$ then $p^2 \nmid s - x$ or $p^t \mid s - x$.

Proof. For each polynomial $q = q_n x^n + \cdots + q_0 \in K[x]$ the following congruence modulo $(s-x)^2$ holds true:

$$\begin{aligned} q \circ s &= q_n \cdot s^n + q_{n-1} \cdot s^{n-1} + \cdots + q_0 \\ &= q_n((s-x)+x)^n + q_{n-1}((s-x)+x)^{n-1} + \cdots + q_0 \\ &\equiv q_n(n \cdot (s-x)x^{n-1} + x^n) + q_{n-1}((n-1)(s-x)x^{n-2} + x^{n-1}) + \cdots + q_0 \\ &= q + q' \cdot (s-x). \end{aligned}$$

In the special case $q = s$ this $\circ$-rule yields

(1) $(s-x)^2 \mid (s \circ s - s) - s' \cdot (s-x) = (s \circ s - x) - (s-x)(s'+1)$.

We may assume $s \neq x$. Write $s - x = p^k r$ where r is prime to p.

Suppose that $p^t \nmid s - x$. Hence $1 \leqslant k < t$. So $p^{k+1} | s \circ s - x$ (as $p^t | s \circ s - x$) and $p^{k+1} \mid (s-x)^2$. Statement (1) implies that $p^{k+1} \mid (s-x)(s'+1)$, hence (2) $p \mid s'+1$ due to the choice of k. We have (3) $s' + 1 = kp^{k-1}p'r + p^k r' + 2$.

As $\mathrm{char}K \neq 2$ statements (2) and (3) yield $k = 1$. □

Corollary 3.9. *Let π be an s-normal mapping and $\mathrm{mip}\pi = p^t$ for an irreducible polynomial p. If $\mathrm{char}K \neq 2$ and $\pi^* - \pi$ is nilpotent (i.e. $p \mid s - x$) then $p^2 \nmid s - x$ (and thus $Vp(\pi)^j = V(\pi^* - \pi)^j$ for all $j \in \mathbb{N}_0$) or $p^t \mid s - x$ (and thus $\pi^* = \pi$).*

Proof. Suppose that $\pi^* \neq \pi$, i.e. $p^t \nmid s - x$. The previous lemma supplies $r \in K[x]$ such that $p \cdot r = s - x$ and r is prime to p. □

Lemma 3.10. *Suppose that* $^- = \mathrm{id}_K$ *and* $\varepsilon = -1$ *and* $\pi : V \to V$ *is linear. Let* U *be a cyclic* π*-module such that (+)* $f(a, b\pi^*) = f(a, b\pi)$ *for all* $a, b \in U$ (*if* $\mathrm{char}K = 2$ *suppose additionally that* $f(a, a) = 0 = f(a, a\pi)$ *for all* $a \in U$). *Then* U *is totally isotropic.*

Observe that (+) holds true when $\pi^* = \pi$.

Proof. When $\mathrm{char}K \neq 2$ then $f(a, a) = 0 = f(a, a\pi)$ for all $a \in V$ follows from the assumptions. We will prove $f(v\pi^m, v\pi^n) = 0$ for all $m, n \in \{0, 1, \ldots\}$ and $v \in V$. If $m = 2i$ and $n = 2j$ we calculate $f(v\pi^m, v\pi^n) = f(v\pi^i\pi^{*j}, v\pi^j\pi^{*i}) = f(v\pi^{i+j}, v\pi^{i+j}) = 0$. If $m = 2i + 1$ and $n = 2j + 1$ we find $f(v\pi^m, v\pi^n) = f(v\pi^{i+j+1}, v\pi^{i+j+1}) = 0$. If $m = 2i + 1$ and $n = 2j$ then $f(v\pi^m, v\pi^n) = f(v\pi^{i+j+1}, v\pi^{i+j}) = f(a\pi, a) = 0$ for $a := v\pi^{i+j}$. □

Proposition 3.11 (**type I modules**, **cyclic case**, f **bilinear**, $\pi^* - \pi$ **nilpotent**). *Let* $\mathrm{char}K \neq 2$. *Let* $V = \langle v \rangle_\pi$ *be a cyclic* π*-module where* π *is s-normal and* $\mathrm{mip}\pi = p^t$ *for an irreducible* p *and* $t \in \mathbb{N}$ (*hence* $\tilde{p} = p$). *Suppose that* $^- = \mathrm{id}_K$ *and* $\pi^* - \pi$ *is nilpotent* (*so* $p \mid s - x$).

If $p^2 \mid s - x$ *then* $\pi^* = \pi$.

(a) *If* $\pi^* = \pi$ *then* $\varepsilon = 1$.

(b) *If* $\varepsilon = 1$ *and* $\pi^* \neq \pi$ *then* t *is odd. If* $\varepsilon = -1$ *then* t *is even.*

Proof. The first assertion repeats Corollary 3.9.

Proof of (a). If $\varepsilon = -1$ and $\pi^* = \pi$ then Lemma 3.10 yields that V is totally isotropic, in contrast to the assumption that (V, f) is regular.

Proof of (b). First consider the symplectic case $\varepsilon = -1$.

If $0 < t \leqslant 2$ then $t = 2$ holds true (else $\pi^* = \pi$ in contrast to (a)). Now let $t \geqslant 3$. The spaces $Vp(\pi)$ and $Vp(\pi)^{t-1}$ are π-modules and π induces on $Vp(\pi)/Vp(\pi)^{t-1}$ a cyclic mapping π' with minimum polynomial p^{t-2}. Further, $\mathrm{rad}(Vp(\pi)) = Vp(\pi)^{t-1}$. So f induces on $Vp(\pi)/Vp(\pi)^{t-1}$ a regular symplectic form and π' is an s-normal mapping on that space. So $Vp(\pi)/Vp(\pi)^{t-1}$ and π' meet the assumptions that were supposed for V and π. By induction $t - 2$ is even. This finishes the symplectic case.

Now let $\varepsilon = 1$ and suppose that $\pi^* \neq \pi$. The bilinear form $h : V \times V \to K$, $h(u, w) := f(u(\pi^* - \pi), w)$ satisfies $h(u, w) = -h(w, u)$ and $\mathrm{rad}(V, h) = \mathrm{kernel}(\pi^* - \pi)$. From $p \mid s - x$ but $p^2 \nmid s - x$ (see Corollary 3.9) we see that $\mathrm{kernel}(\pi^* - \pi) = \mathrm{kernel}p(\pi) = Vp(\pi)^{t-1}$. Hence $V/\mathrm{rad}(V, h)$, endowed with the form induced by h, is a regular symplectic space and π induces an s-normal mapping π' on that space. Further, π' is a cyclic transformation with minimum polynomial p^{t-1}. The assertion in the above yields that $t - 1$ is even. □

Proposition 3.12. (**type I modules**, **non-cyclic case**, **details**) *Let* $\pi : V \to V$ *be an s-normal mapping such that* $\mathrm{mip}\pi = p^t$ *for an irreducible polynomial* p *and* $t \in \mathbb{N}$. *Let* V *be an orthogonally indecomposable but not a cyclic* π*-module.*

Then $V = V_1 \oplus V_2$, *where each* V_i *is a* π*-cyclic module and* $\mathrm{mip}\pi_i = p^t$ *holds true for the restrictions* π_i. *Further,*

(a) $^- = \mathrm{id}_K$

(b) $p \mid s - x$ (*i.e.* $\pi^* - \pi$ *is nilpotent*).

If $\mathrm{char}K \neq 2$ *and* $p^2 \mid s - x$ *then* $\pi^* = \pi$.

If $\mathrm{char}K \neq 2$ *and* t *is odd then* $\varepsilon = -1$ (*so* f *is a symplectic form*).

If charK $\neq 2$ *and* t *is even and* $\pi^* \neq \pi$ *then* $\varepsilon = 1$ (*so* f *is an orthogonal form*).

If $\mathrm{char}K \neq 2$ *and* $\pi^* = \pi$ *then* $\varepsilon = -1$.

(c) *If* $\mathrm{char}K \neq 2$ *then one can achieve that* V_1, V_2 *are totally isotropic.*

Proof. The first assertion follows from Corollary 3.5.

As V is an orthogonally indecomposable π-module but not cyclic $\langle v \rangle_\pi$ is a non-regular subspace for each $v \in V \setminus 0$. Hence

$(*)$ $f(vp(\pi)^{t-1}, v\pi^j) = 0$ for all $v \in V$ and $j \in \mathbb{N}_0$.

Define $h(v,w) := f(v, \overline{w}p(\pi)^{t-1})$. Then $h : V \times V \to K$ is additive in both arguments and $h(\lambda v, w) = \lambda h(v,w)$ and $h(v, \lambda w) = \bar{\lambda} h(v,w)$. Further, $(*)$ yields

$(+)$ $h(v,v) = 0$ for all $v \in V$; hence $h(v,w) = -h(w,v)$. The definition of h entails immediately

$(++)$ $\mathrm{rad}(V,h) = \mathrm{kernel} p(\pi)^{t-1}$.

Proof of (a). The above properties yield $\lambda h(v,w) = \bar{\lambda} h(v,w)$ for all $\lambda \in K$ and $v, w \in V$. As one can take $v, w \in V$ such that $h(v,w) \neq 0$ the assertion follows.

Proof of (b). Statement $(*)$ proves $h(v\pi, v) = 0$, hence $h(v, w\pi) = h(v\pi, w)$ for all $v, w \in V$. As s-normality of π yields $h(v, w\pi) = h(vs(\pi), w)$ we obtain $h(v(s(\pi) - \pi), w) = 0$ for all $v, w \in V$, i.e. $V(s(\pi) - \pi) \subseteq \mathrm{rad}(V,h)$. So $(++)$ implies $p \mid s - x$.

Now let $\mathrm{char} K \neq 2$.

Then Corollary 3.9 yields that $\pi^* = \pi$ or $p^2 \nmid s - x$.

Suppose that $t = 2r + 1$ is odd. Then $f(vp(\pi)^r, vp(\pi)^r) = f(v, vp(\pi)^r \cdot p^*(\pi)^r) = 0$ (due to $p | p^*$ and $(*)$). If $\varepsilon = 1$ then this implies that $Vp(\pi)^r$ is a totally isotropic subspace of V which is impossible (as $r < \frac{1}{2}t$ entails $\dim Vp(\pi)^r > \frac{1}{2}\dim V$). Hence $\varepsilon = -1$.

Now suppose that $t = 2r$ is even and $\pi^* \neq \pi$ and $\varepsilon = -1$.

Put $j(v,w) := f(v(\pi^* - \pi), w)$. Then $j : V \times V \to K$ is a symmetric bilinear form and $R := \mathrm{rad}(V,j) = \mathrm{kernel}(\pi^* - \pi) = \mathrm{kernel} p(\pi)$ (see Corollary 3.9). As $p \mid s - x, p^*$ statement $(*)$ yields $j(vp^{r-1}(\pi), vp^{r-1}(\pi)) = f(v(\pi^* - \pi)p(\pi)^{r-1}p^*(\pi)^{r-1}, v) = 0$, hence $Vp(\pi)^{r-1}$ is a totally isotropic subspace of (V,j). But this does not comply with $\dim Vp(\pi)^{r-1}/R > \frac{1}{2}\dim V/R$.

For the last claim in (b) let $\pi^* = \pi$. If $\varepsilon = 1$ then the symplectic form h (see beginning of the proof) is also symmetric (as $p^*(\pi) = p(\pi)$). Hence $V = \mathrm{rad}(V,h) = Vp(\pi)$ which is not true. □

Proof of assertion (c). We use a lemma that is based on the following theorem (see [20,8,26]).

W.E. Roth's Theorem. Let A be an $n \times n$-matrix, B an $m \times m$-matrix, C an $m \times n$-matrix over a field K (more generally: a commutative ring with 1). The following statements are equivalent.

(i) The matrices

$$\begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

are similar.

(ii) Some $m \times n$-matrix X satisfies $XA - BX = C$.

Lemma 3.13. *Let $f : V \times V \to K$ be a regular symmetric bilinear form and $\pi \in \mathrm{GL}(V)$ a bicyclic[2] self-adjoint mapping. Let S be a cyclic totally isotropic π-module such that $\dim S = \frac{1}{2}\dim V$. Then $V = S \oplus X$ for some totally isotropic cyclic π-module X.*

Proof. Take a totally isotropic subspace Z such that $V = S \oplus Z$. A basis for S and a suitable basis for Z constitute a basis for V such that

$$F = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

is the matrix of f (I denotes a unit-matrix). Then the matrix P of π has the form

$$P = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix},$$

where A is a cyclic matrix. As $\pi = \pi^*$ one has $P = FP^tF^{-1}$, hence $B = A^t$ and $C = C^t$. By our assumption, P is similar to a matrix of the form

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix},$$

[2] That is, V is a direct sum of two proper π-cyclic subspaces.

where D is a cyclic matrix. Hence $\mathrm{char}D = \mathrm{char}A^t$. Also A^t is cyclic. Thus D is similar to A^t and we can assume $D = A^t$. Roth's Theorem (see above) provides a matrix X such that $XA - A^tX = C$. Put $Y := \frac{1}{2}(X^t - X)$ and

$$M = \begin{pmatrix} I & 0 \\ Y & I \end{pmatrix}.$$

Then M is the matrix of an orthogonal mapping (as $MFM^t = F$) and

$$MPM^{-1} = \begin{pmatrix} A & 0 \\ 0 & A^t \end{pmatrix}$$

is the matrix of a mapping $\mu\pi\mu^{-1}$ that leaves S and Z invariant. So π leaves the totally isotropic cyclic π-modules $S\mu^{-1} = S$ and $Z\mu^{-1}$ invariant and one has $V = S \oplus Z\mu^{-1}$. □

Proof of assertion (**c**): *final arguments*

First let us assume that f is symmetric.

We proceed by induction over t. Recall that $t \geqslant 2$. Further, $p^2 \nmid s - x$ (last statement in (b) and Corollary 3.9).

Let $' : Vp(\pi) \to (Vp(\pi))' := Vp(\pi)/Vp(\pi)^{t-1}$ denote the canonical homomorphism. As $(Vp(\pi))^\perp = Vp(\pi)^{t-1}$ the bilinear form f induces on $(Vp(\pi))'$ a regular symmetric bilinear form and π operates as an s-normal mapping π' on $(Vp(\pi))'$.

We have $V = \langle u\rangle_\pi \oplus \langle w\rangle_\pi$ where both cyclic π-modules have minimum polynomial p^t. Hence $(Vp(\pi))' = \langle (up(\pi))'\rangle_{\pi'} \oplus \langle (wp(\pi))'\rangle_{\pi'}$ and p^{t-2} is the minimum polynomial on both π'-cyclic submodules. Each cyclic π-module of V with minimum-polynomial p^t is non-regular. Hence each cyclic π'-module with minimum polynomial p^{t-2} is also non-regular. This implies that $(Vp(\pi))'$ is an orthogonally indecomposable π'-module. By induction we assume that both submodules $\langle (up(\pi))'\rangle_{\pi'}$ and $\langle (wp(\pi))'\rangle_{\pi'}$ are totally isotropic. Then $Vp(\pi) = \langle up(\pi)\rangle_\pi \oplus \langle wp(\pi)\rangle_\pi$ and both π-cyclic submodules $U := \langle up(\pi)\rangle_\pi$ and $W := \langle wp(\pi)\rangle_\pi$ are totally isotropic. Put $\delta := \deg p$.

The form f induces on $U^\perp/U$ a regular symmetric form and π operates as an s-normal mapping π'' on $U^\perp/U$ and $\pi''^* - \pi''$ is nilpotent as $p|s - x$. As $\dim U^\perp/U = 2\delta$ the minimum polynomial is $\mathrm{mip}\pi'' = p$ or $\mathrm{mip}\pi'' = p^2$. But $\mathrm{mip}\pi'' = p^2$ would imply that $U^\perp/U$ is a π''-cyclic module and this is impossible: Proposition 3.11(b) and $p^2 \nmid s - x$. Hence

(1) $U^\perp/U$ is the direct sum of two π''-modules, each with minimum polynomial p, and π'' is a self-adjoint mapping.
Further,

(2) The π''-module $(U \oplus Wp(\pi)^{t-2})/U$ is a totally isotropic submodule of $U^\perp/U$ and it is cyclic with minimum polynomial p.

Due to (1) and (2) $U^\perp/U = (U \oplus Wp(\pi)^{t-2})/U \oplus X/U$ for some π-module X such that X/U is a cyclic π''-module with minimum polynomial p.

We can assume that X/U is totally isotropic; see previous lemma. Then X is a totally isotropic cyclic π-module such that $Xp(\pi) = U$ and its minimum polynomial is p^t.

Similarly we find a totally isotropic cyclic π-module Z such that $Zp(\pi) = W$ and its minimum polynomial is p^t.

If $v \in X \cap Z$ then $vp(\pi) \in U \cap W = \{0\}$, hence $v \in Xp(\pi)^{t-1} \cap Zp(\pi)^{t-1} \subseteq U \cap W = \{0\}$. Hence $X \cap Z = \{0\}$ and $V = X \oplus Z$.

This finishes the proof when f is symmetric.

Now let us assume that f is symplectic.

If $\pi = \pi^*$ then Lemma 3.10 yields that each cyclic π-module is totally isotropic.

Let $\pi^* \neq \pi$. Put $h : V \times V \to K$, $h(u, w) := f(u(\pi^* - \pi), w)$. Then h is a symmetric bilinear form and $\mathrm{rad}(V, h) = Vp^{t-1}$ (second assertion in (b) of the proposition). Further, π induces an s-normal mapping π' on $V/\mathrm{rad}(V, h)$ (we refer to the form induced by h) and $V/\mathrm{rad}(V, h)$ is an orthogonally indecomposable π'-module. The result for the symmetric case provides $V = U \oplus W$ where U and W are cyclic π-modules and $h(U, U) = 0 = h(W, W)$. Hence $f(U(\pi^* - \pi), U) = 0 = f(W(\pi^* - \pi), W)$. Lemma 3.10 entails that $f(U, U) = 0 = f(W, W)$.

The proof of assertion (c) is finished. □

Observation 3.14 (**special case**). Let $\pi^* = \alpha\pi^{-1}$ where $\alpha \in K$ (this includes the case that π is an isometry, i.e. $\alpha = 1$). Let $\mathrm{mip}\pi = p^t$ where p is irreducible and suppose that $\pi^* - \pi$ is nilpotent. If $\alpha = \beta^2$ is a square in K then $p = x - \beta$ or $p = x + \beta$; else $p = x^2 - \alpha$.

In the special case $\alpha = 1$ (i.e. π is a unitary mapping) it follows that $p = x + 1$ or $p = x - 1$ (compare Example 2.12).

Proof. The linear mapping $\alpha\pi^{-1} - \pi = -\pi^{-1}(\pi^2 - \alpha)$ is nilpotent, hence $\pi^2 - \alpha$ is nilpotent. This implies that $p|x^2 - \alpha$. □

Definition 3.15 (**Types of orthogonally indecomposable π-modules**). We give a classification of orthogonally indecomposable π-modules, with some exceptions when $\mathrm{char}K = 2$.

Let $\pi : V \to V$ be an s-normal mapping and suppose that $V \neq 0$ is an orthogonally indecomposable π-module.

Let p denote an arbitrary irreducible polynomial.

Type Ia $\mathrm{mip}\pi = p^t$ and $^- = \mathrm{id}_K$ and $\pi^* - \pi$ is nilpotent and: [$\varepsilon = 1$ and t even and $\pi^* \neq \pi$] or [$\varepsilon = -1$ and t odd and $\pi^* \neq \pi$] or [$\varepsilon = -1$ and $\pi^* = \pi$].

Type Ib $\mathrm{mip}\pi = p^t$ and $^- = \mathrm{id}_K$ and $\pi^* - \pi$ is nilpotent and: [$\varepsilon = 1$ and t odd and $\pi^* \neq \pi$] or [$\varepsilon = -1$ and t even and $\pi^* \neq \pi$] or [$\varepsilon = 1$ and $\pi^* = \pi$].

Type Ic $\mathrm{mip}\pi = p^t$ and [$^- \neq \mathrm{id}_K$ or $\pi^* - \pi$ is not nilpotent].

Type II $\mathrm{mip}\pi = p^t\tilde{p}^t$ where $p \neq \tilde{p}$.

Proposition 3.16. *Let V be an orthogonally indecomposable π-module. If* $\mathrm{char}K = 2$ *assume that* $^- \neq \mathrm{id}_K$ *or that $s - x$ is prime to the minimum polynomial of π.*

Then the orthogonally indecomposable π-module V fits into precisely one of the above four types.

Proof. Clearly π cannot share the properties of two distinct types.

When $\mathrm{char}K = 2$ then V is a type Ic or II module; see Proposition 3.12. Hence we may assume that $\mathrm{char}K \neq 2$.

We claim that π fits into at least one of the types.

If $P(\pi) = \{p, \tilde{p}\}$ where $p \neq \tilde{p}$ then $\mathrm{mip}\pi = p^t\tilde{p}^t$ and type II is present; see Observation 3.3 (c) and Corollary 3.7.

There remains the case $\mathrm{mip}\pi = p^t$. If V is not an indecomposable π-module then Proposition 3.12 ensures that type I,a is appropriate.

If V is an indecomposable π-module and type I,c does not apply then Proposition 3.11 proves that type I,b is present. □

We compile some of the previous results.

Remark 3.17. Let $\mathrm{char}K \neq 2$. An orthogonally indecomposable π-module V of type Ia is a direct sum $V = V_1 \oplus V_2$ of two indecomposable π-modules such that $\mathrm{mip}\pi_i = p^t$ for the restrictions π_i. In particular, V is not a cyclic π-module.

A type II π-module V is a direct sum $V = V_1 \oplus V_2$ of two indecomposable π-modules such that $\mathrm{mip}\pi_1 = p^t$ and $\mathrm{mip}\pi_2 = \tilde{p}^t$ (where $\tilde{p} \neq p$) holds true for the restrictions π_i; in particular, V is a cyclic π-module.

A type Ib and a type Ic π-module V is an indecomposable π-module (in particular a cyclic module).

For further properties see Propositions 3.11 and 3.12.

Remark. The above description of orthogonally indecomposable π-modules reveals coarse relations between K, f and π. We give examples.

When f is an orthogonal or symplectic form ($^- = \mathrm{id}_K$ and $\varepsilon = 1$ respectively $\varepsilon = -1$) and $\pi^* = \pi^{-1}$ then the assumption $p \mid s - x$ and $p = \tilde{p}$ (where $p \in K[x]$ is irreducible) implies that $p = x + 1$ or $p = x - 1$ (see Example 2.12).

If f is orthogonal and anisotropic (i.e. $f(v,v)=0$ holds only true for $v=0$) and char$K\neq 2$ then each orthogonally indecomposable π-module V is a type I,b module or V is a type I,c module with minimum polynomial p (where $p=\tilde{p}$ is prime).

4. Uniqueness statements for orthogonal decompositions

Lemma 4.1. *Let $\pi: V\to V$ be a linear mapping and $V=U\oplus W$ for totally isotropic π-modules U and W. Also let $\pi': V\to V$ be a linear mapping and $V=U'\oplus W'$ for totally isotropic π'-modules U' and W'. The following statements are equivalent.*

(i) *Some isometry $\alpha: V\to V$ satisfies $\pi'=\alpha^{-1}\pi\alpha$ and $U\alpha=U'$ and $W\alpha=W'$.*

(ii) *There is a linear bijection $\beta: U\to U'$ such that $\pi'_{U'}=\beta^{-1}\pi_U\beta$ and $(\pi'^*)_{U'}=\beta^{-1}(\pi^*)_U\beta$ (subscripts denote restrictions).*
Under the additional assumption that π and π' are s-normal mappings for the same $s\in K[x]$ the following statement is also equivalent:

(iii) *Some linear bijection $\beta: U\to U'$ fulfills $\pi'_{U'}=\beta^{-1}\pi_U\beta$.*

Proof. (i) $\Rightarrow$ (ii). Put $\beta:=\alpha_U$. Then $\pi'_{U'}=\beta^{-1}\pi_U\beta$. All $u'\in U'$ and $w'\in W'$ satisfy $f(w',u'\pi'^*)=f(w'\pi',u')=f(w'\alpha^{-1}\pi\alpha,u')=f(w',u'\alpha^{-1}\pi^*\alpha)$. It follows that $(\pi'^*)_{U'}=(\alpha_U)^{-1}(\pi^*)_U\alpha_U=\beta^{-1}(\pi^*)_U\beta$.

(ii) $\Rightarrow$ (i). We want to lift $\beta: U\to U'$ to an isometry $\alpha: V\to V$ such that (1) $W\alpha=W'$ and (2) $\pi'_{W'}=\alpha_W^{-1}\pi_W\alpha_W$. This requires (3) $f(u\beta,w\alpha)=f(u,w)$ for all $u\in U$ and $W\in W$. As (V,f) is regular there is a unique linear mapping $\alpha: V\to V$ satisfying (1) and (3). Then $f(u\alpha,w\alpha)=f(u,w)$ and $f(u\alpha,u_1\alpha)=0=f(u,u_1)$ and $f(w\alpha,w_1\alpha)=0=f(w,w_1)$ for all $u,u_1\in U$ and $w,w_1\in W$. Hence α is an isometry. We claim that (2) holds also true. Indeed, (2) is equivalent to the statement $f(u',w'\pi'_{W'})=f(u',w'\alpha_W^{-1}\pi_W\alpha_W)$ for all $u'\in U'$ and $w'\in W'$, hence (as α is an isometry) to $f(u'(\pi'^*)_{U'},w')=f(u'\alpha_U^{-1}(\pi^*)_U\alpha_U,w')=f(u'\beta^{-1}(\pi^*)_U\beta,w')$. This is equivalent to the second requirement in (ii).

The implication (ii) $\Rightarrow$ (iii) is trivial. Suppose that π and π' are s-normal and (iii) is valid. Then the second identity in (ii) follows: $(\pi'^*)_{U'}=s(\pi'_{U'})=s(\beta^{-1}\pi_U\beta)=\beta^{-1}s(\pi_U)\beta=\beta^{-1}(\pi^*)_U\beta$. □

Proposition 4.2. *Let $s\in K[x]$ and let π and π' be s-normal mappings. If* char$K=2$ *assume that $^-\neq \mathrm{id}_K$ or that $s-x$ is prime to the minimum polynomial of π. Let $V=V_1\perp\cdots\perp V_k$ be an orthogonal decomposition into orthogonally indecomposable π-modules and $V=V'_1\perp\cdots\perp V'_m$ an orthogonal decomposition into orthogonally indecomposable π'-modules.*

Suppose that $\pi'=\alpha^{-1}\pi\alpha$ for some $\alpha\in \mathrm{GL}(V)$ (i.e. π is similar to π').

Then $k=m$. We find a permutation σ on $\{1,\ldots,k\}$ with the following properties. For $i=1,\ldots,k$ the π-type (Ia or Ib or Ic or II; see Definition 3.15) of V_i equals the π'-type of $V'_{i\sigma}$; further, V_i and $V'_{i\sigma}$ have the same minimum polynomial. The mapping α can be chosen such that $\alpha(V_i)=V'_{i\sigma}$ for all i. Additionally, if V_i has type Ia or II then one can achieve that the restriction α_i to V_i is an isometry.

Proof. When char$K=2$ type Ia and Ib π-modules V_i are excluded by our assumptions. First let us assume that V_1 is a type Ia π-module.

Then $V_1=U\oplus W$ where U and W are cyclic π-modules with minimum polynomials p^t and $p=\tilde{p}$ is an irreducible polynomial. We decompose each of the π'-modules $V'_1,\ldots,V'_k$ into a direct sum of indecomposable π'-modules. This supplies a decomposition of V into indecomposable π'-modules. As π is similar to π' the Krull-Remak-Schmidt-Theorem provides an indecomposable π'-module U' in this decomposition such that p^t is the minimum polynomial of the π'-module U'. Then $U'\subseteq V'_{1\sigma}$ for a suitable index 1σ. From $p=\tilde{p}$ it follows that $V'_{1\sigma}$ is not a type II π'-module. As $^-=\mathrm{id}_K$ and $p|s-x$ the type of $V'_{1\sigma}$ is not Ic. Also Ib is impossible (since [$\varepsilon=1$ and t is even] or [$\varepsilon=-1$ and t is odd]). So $V'_{1\sigma}$ is a type Ia π'-module and its minimum polynomial is also p^t.

A similar reasoning applies when V_1 is a type Ib (a type Ic, a type II) π-module: we find some $V'_{1\sigma}$ that is also a type Ib (respectively type Ic, type II) π'-module and the minimum polynomials of both modules coincide.

Analogue arguments apply to $V_2, \ldots, V_k$. This provides an injective mapping $\sigma : \{1, \ldots, k\} \to \{1, \ldots, m\}$ such that V_i and $V'_{i\sigma}$ are π-(respectively π'-) modules of the same type and with the same minimum polynomial for each $i \in \{1, \ldots, k\}$. So $k \leqslant m$, and switching π with π' yields $m \leqslant k$. Hence σ is a permutation.

Now let us assume that V_1 (hence also $V'_{1\sigma}$) is a type Ia or type II π-(respectively π'-) module. Then $V_1 = U \dotplus W$ and $V'_{1\sigma} = U' \oplus W'$ where U and W (U' and W') are totally isotropic (π-respectively π'-) modules (see Proposition 3.12, (c)); and the minimum polynomials are p^t for U and W and also for U' and W'. So some linear bijection $\beta : U \to U'$ satisfies $\pi'_{U'} = \beta^{-1}\pi_U\beta$ (subscripts denote restrictions). Statement (iii) $\Rightarrow$ (i) in the previous lemma supplies an isometry $\alpha_1 : V_1 \to V'_{1\sigma}$ such that $\pi'_1 = \alpha^{-1}\pi_1\alpha$ (where π'_1 denotes the restriction of π' to $V_{1\sigma}$). □

5. Similarity of a transformation to its adjoint

In Observation 1.10 we observed that a linear mapping π is similar to its adjoint π^* under the assumption that $^- = \mathrm{id}_K$.

In an orthogonal group ($\mathrm{so}^- = \mathrm{id}_K$ and $\varepsilon = 1$) each element $\pi \in \mathrm{O}(V,f)$ admits an involution $\sigma \in \mathrm{O}(V,f)$ such that $\pi^\sigma = \pi^{-1}$. This is equivalent to the statement that each $\pi \in \mathrm{O}(V,f)$ is a product $\pi = \sigma\rho$ of two involutions $\sigma, \rho \in \mathrm{O}(V,f)$. We will find a theorem on s-normal mappings that subsumes this fact as a special case.

Lemma 5.1. *Let $\pi : V \to V$ be an s-normal cyclic mapping and $^- = \mathrm{id}_K$. Then $\pi^\sigma = \pi^*$ for a linear mapping σ such that $\sigma^* = \varepsilon\sigma$ and $\sigma^2 = 1_V$.*

Proof. Select a basis $(v, v\pi, \ldots, v\pi^{n-1})$ for V and define the linear mapping $\sigma : V \to V$ such that $v\pi^i\sigma := v(\pi^*)^i$ for $i \in \{0, 1, \ldots, n-1\}$. From $\pi^* = s(\pi)$ and $s \circ s(\pi) = \pi$ it follows that $\sigma^2 = 1_V$. Let $q \in K[x]$. Then $q = r \cdot \mathrm{mip}\pi + p$ for $r, p \in K[x]$ such that $\deg p \leqslant n-1$ or $p = 0$. As $vp(\pi)\sigma = vp(\pi^*)$ by the definition of σ and $\mathrm{mip}\pi = \mathrm{mip}(\pi^*)$ we conclude that $vq(\pi)\sigma = vp(\pi)\sigma = vp(\pi^*) = vq(\pi^*)$, hence $\pi^\sigma = \pi^*$.

Let $u = vq(\pi), w = vm(\pi) \in V$. Then $f(u\sigma, w\sigma) = f(vq(\pi^*), vm(\pi^*)) = f(vm(\pi), vq(\pi)) = \varepsilon f(u,w)$. □

Lemma 5.2. *Let $\pi : V \to V$ be an s-normal mapping and $^- = \mathrm{id}_K$. Suppose that V is an orthogonally indecomposable non-cyclic π-module. Then $\pi^\sigma = \pi^*$ for a linear mapping σ such that $\sigma^* = \varepsilon\sigma$ and $\sigma^2 = 1_V$.*

Proof. Write $V = U \oplus W$ where U and W are π-cyclic modules with minimum polynomials p^t ($p \in K[x]$ irreducible); see Corollary 3.5. As in the proof of the preceding lemma we find an involution $\sigma_U : U \to U$ such that $\pi_U^{\sigma_U} = s(\pi_U)$ and $f(u\sigma_U, u') = \varepsilon f(u, u'\sigma_U)$ for all $u, u' \in U$ ($\pi_U := \pi|_U$). We will define $\sigma_W : W \to W$ such that $\sigma := \sigma_U \oplus \sigma_W$ fulfills (1) $\sigma^2 = 1_V$ and (2) $\pi^\sigma = \pi^*$ and (3) $\sigma^* = \varepsilon\sigma$. Clearly (3) requires

$$(*) \qquad f(u\sigma_U, w) = \varepsilon f(u, w\sigma_W)$$

for all $u \in U$ and $w \in W$. As $W \cap U^\perp = \{0\}$ (else $Wp(\pi)^{t-1} \subseteq \mathrm{rad}(V,f)$) the identity $(*)$ defines an unique linear mapping $\sigma_W : W \to W$. Now we prove that $\sigma := \sigma_U \oplus \sigma_W$ satisfies the properties (1), (2) and (3).

The requirement $(*)$ and $\sigma_U^2 = 1_U$ yield that $f(u, w\sigma_W^2) = f(u,w)$ for all $u \in U$ and $w \in W$, hence $\sigma_W^2 = 1_W$ and thus $\sigma^2 = 1_V$.

The choice of σ_U implies that $\pi_U^{\sigma_U} = s(\pi_U)$. For all $u \in U$ and $w \in W$ the defining identity $(*)$ implies $f(w\sigma_W\pi\sigma_W, u) = f(u\sigma_U, w\sigma_W\pi) = f(u\sigma_U s(\pi)\sigma_U, w\sigma_W) = \varepsilon f(u\sigma_U s(\pi)\sigma_U, w) = \varepsilon f(u\pi, w) = f(ws(\pi), u)$. Hence $\pi_W^{\sigma_W} = s(\pi_W)$. We proved (2).

Finally we prove (3). Take a basis for W and let P denote the matrix of π_W; F the matrix of $f|_{W\times W}$; S the matrix of σ_W. Then $PF = F \cdot s(P)^t$ (as $f(w\pi_W, w') = f(w, w's(\pi_W))$ for all $w, w' \in W$) and $SPS = s(P)$ (as $\sigma_W\pi_W\sigma_W = s(\pi_W)$). This entails the identity (+) $PC = CP^t$ where $C := FS^t$. If (+) holds true for quadratic matrices P, C and if P is a cyclic matrix then $C = C^t$ (a theorem due to Frobenius [5],

rediscovered e.g. in [24]). So $FS^t = SF^t = \varepsilon SF$. This means that $f(w, w'\sigma_W) = \varepsilon f(w\sigma_W, w')$ for all $w, w' \in W$. So $f(w, w'\sigma_W) = \varepsilon f(w\sigma_W, w')$ for all $w, w' \in W$. We proved (3). □

Remark. The lemma does not require charK ≠ 2. Under the assumption charK ≠ 2 a shorter proof is available since we can assume that U and W are totally isotropic subspaces (see Proposition 3.12(c)).

Proposition 5.3. *Let $\pi : V \to V$ be an s-normal mapping and $^- = \mathrm{id}_K$. Then $\pi^\sigma = \pi^*$ for a linear mapping such that $\sigma^* = \varepsilon\sigma$ and $\sigma^2 = 1_V$. Further, $\pi = \sigma\rho$ where $\rho^* = \varepsilon\rho$ and $\rho^2 = \pi\pi^*$.*

Proof. Consider a decomposition $V = \perp V_i$ into orthogonally indecomposable π-modules V_i. It suffices to prove the assertion for the restrictions π_i to V_i. If V_i is a π_i-cyclic module then the assertion follows from Lemma 5.1. Else apply the previous lemma. The assertions on $\rho := \sigma\pi$ follow immediately. □

We give an application of our Proposition 5.3. Suppose that $\mathrm{char}\, K \neq 2$ and f is symplectic (i.e. $^- = \mathrm{id}_K$ and $\varepsilon = -1$). Then $\mathrm{sp}(V,f) = \{\alpha \mid \alpha : V \to V$ is linear and $\alpha^* = -\alpha\}$ is the associated Lie algebra. We claim

Corollary 5.4. *Let* $\mathrm{char} K \neq 2$. *Each element of the symplectic Lie algebra is a commutator* (*in elements of the symplectic Lie algebra*).

Proof. Let $\alpha \in \mathrm{sp}(V,f)$, hence $\alpha^* = -\alpha$. Then α is an s-normal mapping. The previous proposition provides $\sigma \in \mathrm{GL}(V)$ such that $\sigma^2 = 1$ and $\sigma^* = -\sigma$ and $\alpha^\sigma = \alpha^*$. So $2\alpha = \alpha - \alpha^* = \alpha - \alpha^\sigma = \sigma(\sigma\alpha) - (\sigma\alpha)\sigma$ is a commutator in elements of the Lie algebra. □

This improves a result by Hirschbühl [9] that each element of the symplectic Lie algebra is a sum of at most two commutators.

6. Bi-invariant orthogonal decompositions

In this section we assume that the situation of the previous proposition is valid. Additionally we need charK ≠ 2.

Assumption. (C) Let $\mathrm{char} K \neq 2$ and $^- = \mathrm{id}_K$ and $\pi : V \to V$ an s-normal mapping. Let σ be a linear mapping such that $\pi^* = \pi^\sigma$ and $\sigma^* = \varepsilon\sigma$ and $\sigma^2 = 1_V$.

It follows immediately that $\pi = \sigma\rho$ where $\rho^* = \varepsilon\rho$.

We want to generalize a result in [14] (on orthogonal mappings) to s-normal mappings. The claim is that σ can be obtained from the construction underlying the proof of Proposition 5.3. This means, we find an orthogonal decomposition of V into orthogonally indecomposable π-modules such that each π-module is also a σ-module:

Proposition 6.1. *Suppose that assumption* (C) *holds true. Then one finds an orthogonal decomposition $V = \perp V_i$ such that each V_i is an orthogonally indecomposable π-module and also a σ-module.*

The proof requires the following lemma.

Lemma 6.2. *If* $\mathrm{mip}\pi = p^t\tilde{p}^t$ *where p is irreducible and prime to $\tilde{p}$ then one finds some $v \in V$ such that*

(1) *the π-cyclic space $\langle v\rangle_\pi$ is regular,*
(2) *$\langle v\rangle_\pi$ is invariant under π and σ,*
(3) *$\langle v\rangle_\pi$ does not admit a proper orthogonal decomposition into π-modules.*

Proof. Put $U:=V_\pi(p)$ and $W:=V_\pi(\tilde{p})$. Proposition 2.8 yields

(i) $V = U \oplus W$ and U and W are totally isotropic subspaces.

From $p(\pi)^\sigma = p(\pi^*) = p^*(\pi)$ and Corollary 2.6 we conclude

(ii) $U\sigma = W$ and $W\sigma = U$.

(iii) $f(up(\pi)^{t-1}, u\sigma) \neq 0$ for some $u \in U$.

Proof of (iii). Suppose that (iii) fails. Then each pair $u, z \in U$ satisfies $0 = f((u+z)p(\pi)^{t-1}, (u+z)\sigma) = f(up(\pi)^{t-1}, z\sigma) + f(zp(\pi)^{t-1}, u\sigma)$. Hence $f(up(\pi)^{t-1}, z\sigma) = -f(zp(\pi)^{t-1}, u\sigma) = -f(z, u\sigma p^*(\pi)^{t-1}) = -\varepsilon f(z\sigma, u\sigma p^*(\pi)^{t-1}\sigma) = -\varepsilon f(z\sigma, up(\pi)^{t-1}) = -f(up(\pi)^{t-1}, z\sigma)$. As $\mathrm{char}K \neq 2$ we conclude that $f(up(\pi)^{t-1}, z\sigma) = 0$. Together with (ii) and (i) this implies that $Up(\pi)^{t-1} \subseteq W^\perp \cap U \subseteq \mathrm{rad}V$, a contradiction. We proved (iii).

Now select $u \in U$ according to (iii). Put $w:=u\sigma$ and $v:=u+w$. Then $\langle v\rangle_\pi$ is invariant under π and σ. So (2) holds true. Property (ii) implies that the restriction of π to $\langle u\rangle_\pi$ has minimum polynomial p^t. Therefore, the restriction of π to $\langle w\rangle_\pi$ has minimum polynomial $\tilde{p}^t$. As p is prime to $\tilde{p}$ it follows that $\langle v\rangle_\pi = \langle u\rangle_\pi \oplus \langle w\rangle_\pi$. Property (iii) and Lemma 3.4 yield that $\langle v\rangle_\pi$ is a regular and orthogonally indecomposable π-module. □

Proof of the proposition

by induction over $\dim V$.

Let $p \in P(\pi)$. Then $p(\pi)^\sigma = p(\pi^*)$, hence $V_\pi(p)\sigma = V_\pi(\tilde{p})$ (see Corollary 2.6). So each summand $V_\pi(p)$ (where $p \in P$ and $\tilde{p} = p$) respectively $V_\pi(p) \oplus V_\pi(\tilde{p})$ (where $p \in P$ and $\tilde{p} \neq p$) in the orthogonal primary decomposition Proposition 2.8 is invariant under σ. Thus we can assume

(A) $V = V_\pi(p)$ where $p \in P$ and $\tilde{p} = p$, or

(B) $V = V_\pi(p) \oplus V_\pi(\tilde{p})$ where $p \in P$ and $\tilde{p} \neq p$.

Additionally we can assume

$(*)$ If M is a regular π-module which is invariant under σ then $M = 0$ or $M = V$.

Indeed, if M is a non-trivial π- and σ-module then $V = M \oplus M^\perp$ and the induction hypothesis (applied to M and $M^\perp$) supplies the asserted decomposition.

In case (B) Lemma 6.2 yields the assertion. So assume that (A) is valid, $\mathrm{mip}\pi = p^t$ where p is an irreducible monic polynomial with $\tilde{p} = p$. Put $F:=\mathrm{kernel}(\sigma - 1_V)$ (the fixed space of σ) and $N:=V(\sigma - 1)$ (the negative space of the involution σ). As $V = F \oplus N$ we can pick $u \in F \cup N$ such that $up(\pi)^{t-1} \neq 0$. As V is regular one finds $w \in F \cup N$ such that $f(up(\pi)^{t-1}, w) \neq 0$. Both π-cyclic subspaces $U:=\langle u\rangle_\pi$ and $W:=\langle w\rangle_\pi$ are invariant under π and σ. Further, $\mathrm{mip}\pi_U = p^t$ and $\mathrm{mip}\pi_W = p^t$ (use Proposition 2.9). If $U = V$ or $W = V$ the assertion holds true. So let $U, W \neq V$. $(*)$ yields that U and W are non-regular subspaces. From Lemma 3.4 it follows that $U \oplus W$ is a regular orthogonally indecomposable subspace, hence $V = U \oplus W$ by $(*)$. □

References

[1] N. Burgoyne, R. Cushman, Conjugacy classes in linear groups, J. Algebra, 44 (1977) 339–362.
[2] L.E. Dickson, Canonical forms of quaternary abelian substitutions in an arbitrary Galois field, Trans. Amer. Math. Soc. 2 (1901) 103–138.
[3] L.E. Dickson, Memoir on abelian transformations, Amer. J. Math. 26 (1904) 243–318.
[4] D.Z. Doković, J. Patera, P. Winternitz, H. Zassenhaus, Normal forms of elements of classical real and complex Lie and Jordan algebras, J. Math. Phys. 24 (1983) 1363–1373.
[5] G. Frobenius, Über die mit einer Matrix vertauschbaren Matrizen. Sitzungsberichte Preusss. Akad. Wiss. (1910) 3-15.
[6] I. Gohberg, B. Reichstein, On classification of normal matrices in an indefinite scalar product, Integral Equations Operator Theory 13 (1990) 364–394.
[7] O.v. Grudzinski, Supernormal transformations, Unpublished manuscript.
[8] W.H. Gustafson, Roth's Theorem over commutative Rings, Linear Algebra Appl. 23 (1979) 245–251.
[9] R. Hirschbühl, Commutators in classical Lie algebras, Linear Algebra Appl. 142 (1990) 91–111.
[10] B. Huppert, Isometrien von Vektorräumen I, Arch. Math. 35 (1980) 164–176.
[11] B. Huppert, Isometrien von Vektorräumen II, Math. Z. 175 (1980) 5–20.
[12] B. Huppert, Angewandte Lineare Algebra, de Gruyter, Berlin, Heidelberg, New York, 1990.
[13] N. Jacobson, Lectures in Abstract Algebra II, Van Norstrand, New York, 1951.
[14] F. Knüppel, K. Nielsen, On products of two involutions in the orthogonal group of a vector space, Linear Algebra Appl. 94 (1987) 209–216.
[15] W. Landherr, Äquivalenz Hermitescher Formen über einem beliebigen algebraischen Zahlkörper, Abh. Math. Sem. Univ. Hamburg 11 (1935) 245–248.

[16] Ch. Mehl, Essential decomposition of polynomially normal matrices on real indefinite inner product spaces, Electron. J. Linear Algebra 15 (2006) 84–106.
[17] J. Milnor, In isometries of inner product spaces, Invent. Math. 8 (1969) 83–97.
[18] C. Riehm, The equivalence of bilinear forms, J. Algebra 31 (1974) 45–66.
[19] C. Riehm, M.A. Schrader-Frechette, The equivalence of sesquilinear forms, J. Algebra 42 (1976) 495–530.
[20] W.E. Roth, The equations $XA - YB = C$ and $AX - XB = C$ in matrices, Proc. Math. Soc. 3 (1952) 392–296.
[21] R. Scharlau, Zur Klassifikation von Bilinearformen und von Isometrien über Körpern, Math. Z. 178 (1981) 359–373.
[22] T.A. Springer, Over symplectische transformaties, Proefschrift Leiden, 1951.
[23] T.A. Springer, R. Steinberg, Conjugacy classes, 1970 Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69), Lecture Notes in Mathematics, vol. 131, Springer, Berlin, pp. 167–266.
[24] O. Taussky, H. Zassenhaus, On the similarity transformation between a matrix and its transpose, Pacific J. Math. 9 (1959) 893–896.
[25] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Aust. Math. Soc. III (1963) 1–62.
[26] A.J.B. Ward, A straightforward proof of Roth's lemma in matrix equations, Internat. J. Math. Ed. Sci. Tech. 30 (1999) 33–38.
[27] J. Williamson, The equivalence of non-singular pencils of hermitian matrices in an arbitrary field, Amer. J. Math. 57 (1935) 475–490.
[28] J. Williamson, On the algebraic problem concerning the normal forms of linear dynamical systems, Amer. J. Math. 58 (1936) 141–163.
[29] J. Williamson, On the normal forms of linear canonical transformations in dynamics, Amer. J. Math. 59 (1937) 599–617.
[30] J. Williamson Normal matrices over an arbitrary field of characteristic zero, Amer. J. Math. 61 (1939) 335–356.
[31] J. Williamson, Note on the equivalence of nonsingular pencils of hermitian matrices, Bull. Amer. Math. Soc. 61 (1945) 894–897.
[32] M.J. Wonenburger, Transformations which are products of two involutions, J. Math. Mech. 16 (1966) 327–338.
[33] H. Zassenhaus, On a normal form of the orthogonal transformation I, II, III, Can. Math. Bull. 1 (1958) 31–39, 101–111, 183–191.